ALCUNE INFOMAZIONI UTILI SUL GDPR

Cosa è il GDPR?

Il **Regolamento Generale sulla Protezione dei Dati**, ufficialmente regolamento (UE) n. 2016/679 in sigla RGPD (più noto con la sigla inglese **GDPR**), è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, **operativo a partire dal 25 maggio 2018**.
Il Regolamento è direttamente applicabile in tutti i 28 Stati membri dell'Unione europea. Ogni trattamento, dalla raccolta alla elaborazione, dalla conservazione alla distruzione di un dato, indipendentemente dalle modalità con il quale venga effettuato, sarà soggetto al GDPR.

Cosa si intende per dato personale ?

Il dato personale, come definito dal GDPR, è "**qualsiasi informazione riguardante una persona fisica identificata o identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Chi si deve adeguare?

Tutti i soggetti, **dal professionista alla grande Azienda**, che trattano dati personali attraverso processi tradizionali e automatizzati.
Non rientrano invece le attività a carattere personale o domestico senza connessione con un'attività commerciale o professionale.
L'applicazione del regolamento sulla privacy è una cosa complessa che richiede una attenta analisi della tua struttura. **Trattare in maniera superficiale il GDPR può essere molto rischioso** sopratutto per i responsabili.

Cosa si rischia?

Violare il Regolamento può portare a diverse conseguenze sul piano sanzionatorio. Si rischia infatti di incorrere in sanzioni economiche **fino a 20 milioni di euro o al 4% del fatturato annuale**.
Le sanzioni saranno ovviamente inflitte sulla base di vari fattori come la natura, la gravità e la durata dell'inadempienza.
Le sanzioni più serie sono previste per coloro i quali non rispettano i principi basilari in materia di trattamento dei dati personali.

Cosa è il registro delle attività di trattamento?

L'art. 30 del GDPR prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del **registro delle attività di trattamento**. E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento (sul registro del responsabile).
Costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.
Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

(fonte: www.garanteprivacy.it)

Kepler Informatica S.n.c.
Via Ticino, 5 20061 Carugate (MI) - P.Iva 03405250964
www.keplerinformatica.it

ALCUNE INFOMAZIONI UTILI SUL GDPR

Chi è tenuto a redigerlo ?

Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento (Art. 30, par. 1 e 2 del GDPR). In particolare, in ambito privato, i soggetti obbligati sono così individuabili:

- imprese o organizzazioni con **almeno 250 dipendenti**;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui **trattamenti che possano presentare un rischio**, anche non elevato, per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui **trattamenti non occasionali**;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui **trattamenti delle categorie particolari di dati** di cui all'articolo 9, paragrafo 1 GDPR, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 GDPR.

Rientrano nella categoria delle "organizzazioni" di cui all'art. 30, par. 5 anche le associazioni, fondazioni e i comitati.

Alla luce di quanto detto sopra, sono tenuti all'obbligo di redazione del registro, ad esempio:

- **esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente** (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- **liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati** (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- **associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati** (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- **il condominio ove tratti "categorie particolari di dati"** (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Infine, si precisa che le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del GDPR, **il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento**, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il **principio di accountability** e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

(fonte: www.garanteprivacy.it)